



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/364,835	07/30/1999	BAIJU V. PATEL	INTL-0182-US	9974

7590 03/27/2003

TIMOTHY N TROP  
TROP PRUNER HU & MILES PC  
8554 KATY FREEWAY  
SUITE 100  
HOUSTON, TX 77024

EXAMINER

HA, LEYNNA A

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 03/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/364,835

Applicant(s)

PATEL ET AL.

Examiner

LEYNNA T. HA

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. Suggestion to modify the title.
2. Claims 21-27 are rejected under 35 U.S.C 101.
3. Claims 1-12 and 16-20 are rejected under 35 U.S.C 102(e) with consideration to the prior art's filing date of June 19, 1998.
4. Claims 13-15 and 21-27 are rejected under 35 U.S.C 103(a).

***Specification***

5. **The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.**

**The following title is suggested:** "A Method and Article for Processing Cryptographic Services of Data in a Network System"

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

**6. The claimed invention is directed to non-statutory subject matter.**

**See MPEP 2107-2107.02.**

The invention as recited in claims 21-27 are directed to a device coupled to a communications channel comprising “an entity” and a “controller”. Examiner asserts that an entity and a controller can be considered a hardware-based or entirely software-based, wherein, an entity can be a device that generates data or a software to instruct data generation to transmit to the communications channel and a controller can be a hardware component or in software form to control communication. However, the specification fails to clearly discuss an entity and a controller as being hardware or software-based. Therefore, these claims are rejected as being directed to non-statutory subject matter.

For purposes of applying art, the Examiner, gives the broadest reasonable interpretation of the claimed language for an entity (that generates data) and a controller (that controls data communication) as software.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

***7. Claims 1-12 and 16-20 are rejected under 35 U.S.C. 102(e) as being unpatentable by Nikander, et al. (US 6,253,321).***

**As per claim 1**, Nikander discloses a method where a network is connected to a gateway device to implement packet transformations (col.4, lines 24-27) according to the filter code and security association. Examiner asserts that the filter codes determine the security service that can be performed to a data block (packet) (col.7, lines 65-67). Nikander determines the operations of the incoming and/or outgoing packets (col.4, lines 28-37) according to the filter code and generating security information, whereby, the Examiner asserts the

security information is in the form of security associations. Security associations are information that identifies the type of transformation on the packet (col.6, lines 60-67). The microprocessor or a controller (col.9, lines 20-30) performs packet per packet processing (col.5, lines 21-27) according to the filter code.

**As per claim 2**, Nikander processing includes cryptographic processing to the packets (col.5, lines 21-27).

**As per claim 3**, Nikander discusses a software routine that involves a filter code mechanism containing filter codes that are executable processor instructions that are sent (col.8, lines 57-60) and is stored in the operating system kernel (col.8, lines 12-14). Further, a filter code is the core of the control logic (of an IPSEC engine) that controls processing of incoming and outgoing packets and controls the application transforms applied to the data packets (col.4, lines 40-45).

**As per claim 4**, Nikander discloses a filter code making policy decisions such as determining whether to drop or pass the data packet without applying transformations (col.4, lines 41-52). The IPSEC engine of the microprocessor performs packet transformations, which involves cryptographic transformations on the packets (col.9, lines 20-30). Thus, the Examiner asserts the microprocessor cannot perform the security service for the data packet once it is determined that the data packet is passed without applying transformations because cryptographic transformation occurs in the IPSEC of

the microprocessor. Instead, the application of the filter code (as discussed in claim 3) processes the packet (col.7, lines 55-57).

**As per claim 5**, Nikander's invention is according to the Internet Protocol security protocol also known as IPSEC protocol (col.9, lines 8-10).

**As per claim 6**, Nikander discloses a method with a device that includes a microprocessor adapted to receive and transmit information with a transport medium in the form of a network (col.9, lines 18-20) to implement packet transformations (col.4, lines 24-27). Nikander discusses the filter code receiving the data packets (col.4, lines 40-45), sending it to the microprocessor (col.9, lines 20-30) to perform packet per packet processing where cryptographic processing on packets occurs (col.5, lines 21-27), and outputting the processed data (col.7, lines 56-57).

**As per claim 7**, Nikander discusses the reprocessing of the packet by the microprocessor where the Examiner asserts that reprocessing is performing cryptographic processing more than once (col.7, lines 26-33).

**As per claim 8**, Nikander discloses a method with a device that includes a microprocessor adapted to receive and transmit information with a transport medium in the form of a network (col.9, lines 18-20) to implement packet transformations (col.4, lines 24-27). Nikander teaches simple operations that can be executed quickly where the filter code uses the comparison result from comparing a field or a portion in the packet header against the known value, to determine the process of the packet whether to apply a transformation or to

pass the packet in its current form (col.8, lines 15-20). If a transformation applies to the packet, then the microprocessor performs cryptographic processing on packet (col.5, lines 21-27).

**As per claim 9**, Nikander discloses an IPSEC engine in the microprocessor to perform cryptographic processing (col.5, lines 25-28).

**As per claim 10**, is rejected on the same basis as claim 4.

**As per claim 11**, Nikander discloses a network connected to a system that includes a microprocessor for processing the data and a core memory for storing the operating system kernel containing filter codes that are executable processor instructions (col.8, lines 12-14 and 57-60) that identifies the security service to be performed on a data packet (col.7, lines 65-67).

**As per claim 12**, Nikander discloses a filter code making policy decisions such as determining whether to drop or pass the data packet without applying transformations (col.4, lines 41-52). The IPSEC engine of the microprocessor performs packet transformations, which involves cryptographic transformations on the packets (col.9, lines 20-30). Thus, the Examiner asserts the microprocessor cannot perform the security service for the data packet once it is determined that the data packet is passed without applying transformations because cryptographic transformation occurs in the IPSEC of the microprocessor. Instead, the application of the filter code (as discussed in claim 3) processes the packet (col.7, lines 55-57).



**As per claim 16**, Nikander includes a receiving circuit in the form of the packet interceptor that sees every IP packet or packets according to other protocol in the network and separates these packets to pass to the IPSEC engine wherein cryptographic processing occurs (col.5, lines 42-48).

**As per claim 17**, Nikander includes a core memory for storing the filter codes that identifies the security service to be performed on a data packet (col.7, lines 65-67) and further, the filter code uses the comparison result after comparing a field or a portion in the packet header against the known value to determine the transformation process of the packet according to its security association (col.8, lines 15-20).

**As per claim 18**, Nikander discusses updating data transmission statistic for every packet such as new security associations being established (col.6, lines 50-58) and new compiled filter code (col.7, lines 61-63) are stored in the IPSEC engine of the core memory (col.9, line 30).

**As per claim 19**, the Examiner asserts updating the information based on the predetermined replacement policy is updating the information (such as the security association) when the lifetime expires as disclosed by Nikander.

**As per claim 20**, Nikander discusses the security association (col.6, lines 61-67 and col.7, lines 4-9).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**8. *Claims 13-15 and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikander.***

**As per claim 13**, differs from claim 11 where Nikander implicitly disclose the process of determining the status of the packet whether to apply a transformation (security service) or to pass the packet in its current form (col.8, lines 15-20). If a transformation applies to the packet, then the microprocessor performs cryptographic processing on the packet (col.5, lines 21-27).

Examiner asserts since the microprocessor performs packet per packet processing, that each data packet would be examined and processed accordingly (col.5, lines 42-49). It is motivated to include a filter code and a security association to the data packets so that each packet gives some kind of indication that the packet has undergone a transformation (col.6, lines 60-67). It would have been obvious that each data packet has an indicator, such as the filter code and the security association, to provide information to the

microprocessor whether or not to apply an IPSEC transform on a packet (col.7, lines 42-67).

**As per claim 14**, Nikander implicitly teaches executing instructions to the system to retrieve the filter code and the security association from a policy database (col.5, lines 30-40) in order to send along with the data packet to the microprocessor to perform a cryptographic transformation.

**As per claim 15**, Nikander includes an operating system kernel containing filter codes that are executable processor instructions (col.8, lines 12-14 and 57-60) that identify the security service to be performed on a data packet (col.7, lines 65-67).

**As per claim 21**, Nikander discloses a device that provides security for data transmission through an IPSEC standard and a controller including an engine for modifying the data before transmitting to the Internet. However, Nikander implicitly includes an entity that generates data for transmission wherein the Nikander device has the ability to perform operations on incoming and/or outgoing packets and applying transforms to the packets (col.4, lines 25-45). Examiner asserts the outgoing packets are generated packets in the form of input packets. Nikander discusses the input packets are transformed into output packets that the user wants to send to another user through the Internet (col.1, lines 57-65). Examiner also asserts to modify the data is to change the data from its original form by a cryptographic process (encrypting and/or decrypting the data) and thereafter applying a transform that data

packet according to the IPSEC standard before transmitting package (col.5, lines 25-67).

**As per claim 22**, Nikander discusses the engine performing cryptographic processing (col.5, lines 25-67).

**As per claim 23**, Nikander includes a network controller in the form of a microprocessor (col.9, lines 19-20).

**As per claim 24**, Nikander implicitly discloses an entity includes an application process (i.e. an electronic mail application) that transforms the input packets into output packets to send through the Internet (col.1, lines 57-65). As understood by the examiner, an application process can be in the form of an electronic mail application where its function is to send secure e-mails over the Internet. The use of transmitting secure e-mails through the Internet is well known in the art and takes Official as such. It is motivated to include an e-mail application with Nikander is to be able to transmit the e-mail in a secure manner by applying a cryptographic transform according to the security protocol. Therefore, it would have been obvious to modify Nikander by including an e-mail application in order to send e-mails securely over the Internet.

**As per claim 25**, as rejected on the basis of claim 14.

**As per claim 26**, Nikander includes a receiving circuit in the form of the packet interceptor that sees every IP packet or packets according to other protocol in the network and separates these packets to pass to the IPSEC

engine wherein the filter code identifies if cryptographic processing occurs (col.5, lines 42-48).

**As per claim 27**, as rejected on the same basis as claim 22.

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Friday (7:00 - 3:30PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, GAIL O. HAYES can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

L. HA  
March 19, 2003



GAIL HAYES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100